REN-ISAC and the Shared Darknet Project

Boston University Security Camp

March 2006

Doug Pearson

REN-ISAC

- Is an integral part of U.S. higher education's strategy to improve network security through information collection, analysis, dissemination, early warning, and response;
- is specifically designed to support the unique environment and needs of organizations connected to served higher education and research networks; and
- supports efforts to protect the national cyber infrastructure by participating in the formal U.S. ISAC structure.

REN-ISAC Activities

- Build a trust community for R&E cybersecurity professionals
- Information products
- Provide information-sharing / communications channels
- Incident response
- 24x7 Watch Desk
- Developing R&E Cybersecurity Contact Registry
- Security work in specific communities, e.g. grids
- Participate in other higher education efforts
- Participate in mitigation communities

Information Products

- The **Daily Weather Report**, sent to members, provides an aggregate-level analysis aimed to help situational awareness and to provide actionable protection information.
- **Alerts**, sent to members, provide critical actionable protection information. Unique information gained from our monitoring, analysis, or relationships; or value-add to existing info.
- **Notifications**, sent to individual institutions (members and non-members) identify specific sources of active threat at the institution. Intelligence comes from our sensors, direct reconnaissance, and from information shared by members or gained in other sharing relationships.
- Views of information from our **Monitoring** systems

Activities and Information Products

- New services in the works:
  - Secure web-based lists of botnet c&c, malware sites, etc.
  - Active information channels
    - Member information sharing
    - Real-time communications channel
  - REN-ISAC Tech Bursts webcasts
  - Shared Darknet Project
- New services under consideration
  - HoneyFarm with distributed EDU address space.
  - SMS alerts
- We like feedback! Comments about improving existing services or useful new services to ren-isac@iu.edu.

REN-ISAC Membership

- A trusted community for sharing sensitive information regarding cybersecurity threat, incidents, response, and protection, specifically designed to support the unique environment and needs of higher education and research organizations.
- Membership is oriented to permanent staff with organization-wide responsibility for cybersecurity protection or response at an institution of higher education, teaching hospital, research and education network provider, or government-funded research organization.
- http://www.ren-isac.net/membership.html

REN-ISAC Membership

- Without membership you'll still receive Notifications.
- With membership, you'll
  - get plugged into the vetted trust community,
  - participate in the information sharing,
  - receive our information products including the Daily Weather Report and Alerts,
  - receive notifications from our darknet monitor,
  - be able to participate in the Shared Darknet Project, and
  - participate in other channels and projects we have in the works
- http://www.ren-isac.net/membership.html

Shared Darknet Project

- The aim of the Shared Darknet Project is to develop a wide-aperture, powerful network security sensor that will directly serve higher-education and research institutions, and indirectly serve Internet users at large.
- To participate in the Shared Darknet Project, institutions who run local darknets send their collector data (only the hits coming from outside their institution) to REN-ISAC. The data is analyzed to identify compromised machines by IP address, destination ports involved, the number of "hits" seen, and timestamps of the activity.
- The REN-ISAC compiles the darknet data contributions and creates two distinct information products: notifications and reports.

Shared Darknet Project

- Notifications identify specific compromised machines and are sent to the security contact at the institution owning the source address, except by mutual agreement otherwise. Notifications will be sent regardless of whether the institution is a participant in the Shared Darknet Project or not.
- Notifications of compromised hosts from commercial and other organizations will be forwarded in aggregate to relevant private network security collaborations.
- Reports are sent to all [REN-ISAC members(?) / participants in the Shared Darknet project(?)]. Reports contain data about trends within the Shared Darknet based on the aggregate data from all sensors. These reports provide greater details and provide each participant with a broader perspective than is available from only their local darknet data.

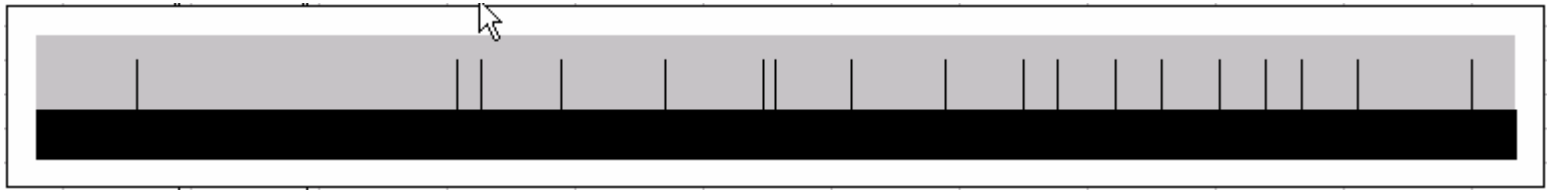
SDP - Benefits

- Wide aperture (large amount of IP address space widely distributed) = a more powerful sensor than a standalone system
- Resilient to counterintelligence = difficult for miscreants to identify and intentionally avoid the darknet
- Combined brainpower.
- An excellent picture of what's affecting higher ed.
- Will enable substantial progress in combating worms and other malicious activity that relies on scanning for vulnerable systems.

Shared Darknet Project - Why

One lonely /16 darknet in the entire IPv4 space,
(actually the /16 line should be ~10x skinnier!)

versus a Shared Darknet Project



Darknet R&D and Opportunity Areas

- Trend analysis - best techniques and methods
- Noise reduction, e.g. P2P NAT and firewall traversal methods
- New ways of representing of results
  - e.g. http://www.monkey.org/~phy/ipmaps/darknet.php
- Payload analysis
- Information sharing - what's the best way to compile observations and feed them to an institution's incident ticketing system?

- SDP work is being organized in cooperation with the SALSA CSI2: http://security.internet2.edu/csi2/

Darknets

- Some examples of darknet systems are:
  - http://www.cymru.com/Darknet/index.html
  - http://ims.eecs.umich.edu/

To Join the SDP

- Project not quite off the ground yet
  - Need to finish a data sharing MOU template
  - Finalize the scripts and transfer method (secure copy)
  - Finish project documents, e,g how-tos, etc.
  - Anticipate first participants on-line in early April
- In the meantime
  - Join the R-I darknet discussion mailing list; send e-mail to ren-isac@iu.edu
- The R-I darknet discussion mailing list is open only to REN-ISAC members, and is open to all members, regardless of participation in the SDP.

Contacts

Research and Education Networking ISAC
http://www.ren-isac.net
24x7 Watch Desk: +1(317)278-6630
ren-isac@iu.edu

Membership: http://www.ren-isac.net/membership.html

Doug Pearson
dodpears@iu.edu